

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
6 décembre 2001 (06.12.2001)

PCT

(10) Numéro de publication internationale  
**WO 01/93528 A2**

(51) Classification internationale des brevets<sup>7</sup> : **H04L 29/06**

(72) Inventeur; et

(21) Numéro de la demande internationale :

PCT/FR01/01623

(75) Inventeur/Déposant (pour US seulement) : **GIRARD, Pierre** [FR/FR]; 4 avenue Brue, F-13600 La Ciotat (FR).

(22) Date de dépôt international : 25 mai 2001 (25.05.2001)

(74) Mandataire : **MILHARO, Emilien**; c/o GEMPLUS, Av du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos (FR).

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :  
00/07180 31 mai 2000 (31.05.2000) FR

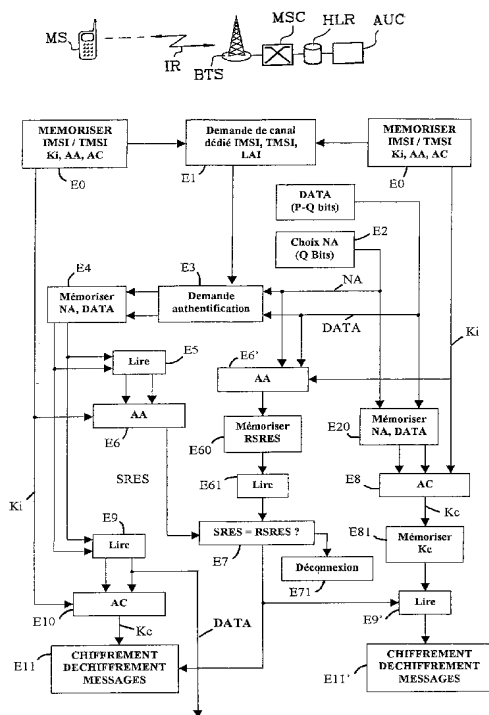
(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(71) Déposant (pour tous les États désignés sauf US) : **GEMPLUS** [FR/FR]; Avenue Pic de Bertagne, Parc d'activités de Gémenos, F-13881 Gémenos (FR).

[Suite sur la page suivante]

(54) Title: METHOD FOR SECURE COMMUNICATION BETWEEN A NETWORK AND A TERMINAL SMART CARD

(54) Titre : PROCEDE DE COMMUNICATION SECURISEE ENTRE UN RESEAU ET UNE CARTE A PUCE D'UN TERMINAL



E0...STORE IMSI/TMSI, K<sub>i</sub>, AA, AC  
E1...REQUEST IMSI/TMSI, LAI DEDICATED CHANNEL  
E2...SELECT NA (Q BITS)  
E3...REQUEST AUTHENTICATION  
E4...STORE NY, DATA  
E5...READ  
E60...STORE RSRES  
E20...STORE NA, DATA

E61...READ  
E9...READ  
E11...MESSAGE ENCRYPTION/DECRYPTION  
E71...DISCONNECT  
E81...STORE KC  
E9'...READ  
E11'...MESSAGE ENCRYPTION/DECRYPTION

(57) Abstract: The invention concerns a method which sets up a secure transmission between two entities in a telecommunication network, and particularly between a mobile terminal (MS) and the stationary network, in particular visitor locating and home location registers (VLR, HLR) and an authenticating centre (AUC), in a cellular radiotelephone network. During authentication (E9, E9', E10) of a terminal, and more precisely of the SIM card therein, the data DATA are transmitted by the stationary network with a random number (NA) produced by the stationary network. The data DATA, the random number NA and a key (K<sub>i</sub>) are applied in the first and second entities to an algorithm (AA) to proceed with authentication.

(57) Abrégé : Le procédé établit un canal de transmission sécurisé entre deux entités dans un réseau de télécommunication, et particulièrement entre un terminal mobile (MS) et le réseau fixe, notamment des enregistreurs de localisation des visiteurs et nominal (VLR, HLR) et un centre d'authentification (AUC), dans un réseau de radiotéléphonie cellulaire. Au cours de l'authentification (E9, E9', E10) du terminal, et plus précisément de la carte SIM dans celui-ci, les données DATA sont transmises par le réseau fixe avec un nombre aléatoire (NA) produit par le réseau fixe. Les données DATA, le nombre aléatoire NA et une clé (K<sub>i</sub>) sont appliqués dans les première et deuxième entités à un algorithme (AA) pour procéder à l'authentification.

WO 01/93528 A2



**(84) États désignés (régional) :** brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

*En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.*

**Publiée :**

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

**Procédé de communication sécurisée entre un réseau et  
une carte à puce d'un terminal**

La présente invention concerne un procédé de  
5 communication sécurisée entre une carte à puce d'un  
terminal radiotéléphonique mobile MS et un sous-  
système d'acheminement, appelé souvent réseau fixe,  
dans un réseau de radiotéléphonie cellulaire  
numérique. Plus particulièrement, l'invention  
10 instaure un canal de communication sécurisé à travers  
l'interface radio entre une carte ou module à  
microprocesseur, dite carte à puce SIM (Subscriber  
Identify Module), amovible du terminal, et un centre  
d'authentification du réseau de radiotéléphonie.

15

Un réseau de radiotéléphonie cellulaire  
numérique RR de type GSM, auquel référence sera faite  
dans la suite à titre d'exemple, comprend  
principalement plusieurs terminaux radiotéléphoniques  
20 mobiles MS et un réseau fixe proprement dit où  
circule notamment des messages de signalisation, de  
contrôle, de données et de voix comme montré  
schématiquement à la figure 1.

25 Dans le réseau RR montré à la figure 1 sont  
représentées notamment des entités principales à  
travers lesquelles des données destinées à la carte  
SIM d'un terminal mobile MS situé dans une zone de  
localisation à un instant transigent. Ces entités  
30 sont un commutateur du service mobile MSC relié à au  
moins un commutateur téléphonique à autonomie  
d'acheminement CAA du réseau téléphonique commuté RTC  
et gérant des communications pour des terminaux  
mobiles visiteurs, parmi lesquels le terminal MS, qui  
35 se trouvent à un instant donné dans la zone de  
localisation respective desservie par le commutateur

MSC. Un enregistreur de localisation des visiteurs VLR est relié au commutateur MSC et contient des caractéristiques, telles qu'identité et profil d'abonnement des terminaux mobiles, en fait des cartes SIM dans ceux-ci, situés dans la zone de localisation. Un contrôleur de station de base BSC relié au commutateur MSC gère notamment l'allocation de canaux à des terminaux mobiles, la puissance de station(s) de base et des transferts intercellulaires de terminaux mobiles. Une station de base BTS reliée au contrôleur BSC couvre la cellule radioélectrique où le terminal MS se trouve à l'instant donné.

Le réseau de radiotéléphonie RR comprend encore un enregistreur de localisation nominal HLR coopérant avec un centre d'authentification AUC et relié aux commutateurs du service mobile à travers le réseau de signalisation du réseau de radiotéléphonie RR. L'enregistreur HLR est essentiellement une base de données, comme un enregistreur VLR, qui contient pour chaque terminal MS l'identité internationale IMSI (International Mobile Subscriber Identity) de la carte SIM du terminal, c'est-à-dire de l'abonné possesseur de la carte SIM, le numéro d'annuaire et le profil d'abonnement de l'abonné, et le numéro de l'enregistreur VLR auquel est rattaché le terminal mobile et mis à jour lors de transferts entre zones de localisation.

Le centre d'authentification AUC assure l'authentification des abonnés et participe à la confidentialité des données transitant dans l'interface radio IR entre le terminal MS et la station de base BTS auquel il est rattaché à l'instant donné. Il gère un algorithme d'authentification A3 et un algorithme A8 de

détermination de clé du chiffrement, parfois fusionnés en un seul algorithme A38, selon la norme GSM, qui sont redondants dans la carte SIM du terminal mobile MS, préalablement à toute communication avec le terminal, ou bien lors de la mise en fonctionnement du terminal ou lors d'un transfert intercellulaire. En particulier, le centre d'authentification AUC mémorise une clé d'authentification Ki attribuée uniquement à l'abonné en correspondance avec l'identité IMSI de l'abonné mémorisée dans l'enregistreur de localisation nominal HLR lors de la souscription d'abonnement par l'abonné.

Dans un réseau de radiotéléphonie numérique de type GSM, représenté à la Figure 1, il est très important d'authentifier le terminal radiotéléphonique mobile MS pour, entre autre, pouvoir reconnaître l'abonné. Afin d'assurer une flexibilité maximale, le centre d'authentification n'authentifie pas le terminal mobile MS lui-même mais la carte à puce SIM qu'il contient. Cette carte contient la clé Ki attribuée à l'abonné et prouve au moyen de l'algorithme d'authentification A3 qu'elle connaît la clé sans la révéler. Le réseau fixe envoie un nombre aléatoire RAND (challenge) à la carte et demande à la carte d'entrer le nombre aléatoire et la clé dans l'algorithme d'authentification pour un calcul cryptographique et de lui retourner le résultat sous la forme d'une réponse signée SRES (Signed RESponse) pour la norme GSM. Il est très difficile à un "attaquant", une tierce personne malveillante souhaitant établir des communications radiotéléphoniques débitées sur le compte du propriétaire de la carte SIM, de prévoir la valeur du nombre aléatoire. Sans la connaissance de la clé,

l'attaquant ne peut pas contrefaire une réponse. La taille du nombre aléatoire empêche l'attaquant de garder en mémoire toutes les valeurs du couple nombre aléatoire-réponse signée dans un dictionnaire. La

5      procédure d'authentification dans le réseau de radiotéléphonie authentifie ainsi la carte SIM contenant une clé.

La procédure d'authentification, représentée à

10      la figure 2, comprend brièvement les étapes suivantes:

- préalablement, le centre d'authentification AUC choisit plusieurs nombres aléatoires RAND et

15      détermine d'une part plusieurs réponses de signature RSRES respectivement en fonction des nombres choisis RAND et de la clé Ki attribuée à l'abonné appliqués à l'algorithme d'authentification A3, et d'autre part plusieurs clés de chiffrement respectivement en

20      fonction des nombres choisis RAND et de la clé Ki appliqués à l'algorithme de détermination de clé A8, afin de fournir des triplets [nombre aléatoire RAND, réponse de signature SRES, clé de chiffrement Kc] à l'enregistreur de localisation HLR, dès la

25      souscription d'abonnement au service de radiotéléphonie mobile, puis chaque fois que l'enregistreur HLR a épuisé sa réserve de triplets, en correspondance avec l'identité IMSI de la carte SIM de l'abonné ;

30

- chaque fois que l'enregistreur de localisation des visiteurs VLR auquel est rattachée momentanément la carte SIM demande une authentification de la carte, l'enregistreur HLR choisit et fournit au moins

35      un triplet à l'enregistreur VLR afin de transmettre

le nombre aléatoire du triplet choisi à la carte SIM à travers le réseau fixe et le terminal mobile MS ;

5           - la carte SIM effectue un calcul cryptographique en appliquant le nombre aléatoire transmis et la clé Ki à l'algorithme d'authentification A3 produisant la réponse signée SRES et la retourne à l'enregistreur VLR ;

10           - l'enregistreur VLR compare la réponse signée SRES à celle contenue dans le triplet choisi, et en cas d'égalité des réponses, la carte est authentifiée.

15           Les réseaux de téléphonie cellulaire numérique existants de type GSM ne disposent pas d'un canal de transmission de données sécurisé assurant la confidentialité et l'intégrité des données transmises tout en assurant simultanément l'impossibilité de  
20           dénis de service.

          En effet, des services d'envoi de message SMS (Short Message Services) ont été définis, mais ils ne procurent aucune certitude quant à la réception des  
25           données, et ne garantissent donc pas l'impossibilité d'un dénis de service.

          Or dans de nombreux cas, il est nécessaire de pouvoir transmettre des données DATA en assurant leur  
30           intégrité, leur confidentialité et l'impossibilité d'un dénis de service, la plupart du temps pour des raisons de sécurité.

          L'invention vise à remédier aux inconvénients  
35           exposés ci-dessus, sans modifier le matériel du réseau de radiotéléphonie et avec quelques

modifications de logiciel en relation essentiellement avec l'authentification.

5 A cette fin, un procédé de transmission sécurisée de données (DATA) entre une première entité (MS) et une deuxième entité (VLR, HLR, AUC) dans un réseau de télécommunication (RR), comprenant une étape d'authentification de la première entité (MS) par la seconde entité (VLR, HLR, AUC), ladite étape  
10 d'authentification comprenant des étapes (E6, E6') d'appliquer une clé (Ki) mémorisée dans les première et deuxième entités et un nombre aléatoire (NA) produit par la deuxième entité et transmis par la deuxième entité à la première entité à des  
15 algorithmes identiques (AA) mémorisés dans les première et deuxième entités, et comparer (E7) dans la deuxième entité (VLR, HLR, AUC) une réponse (SRES) produite par l'algorithme (AA) mémorisé dans la première entité et transmise à la deuxième entité et  
20 un résultat de réponse (RSRES) produit par l'algorithme (AA) mémorisé dans la deuxième entité, est caractérisé par les étapes de transmettre de la deuxième entité à la première entité les données (DATA) avec le nombre aléatoire (NA), appliquer les  
25 données (DATA) avec le nombre aléatoire (NA) à l'algorithme (AA) dans la première entité et dans la seconde entité.

Lorsque l'authentification est terminée, le  
30 réseau RR est certain que les données DATA sont bien parvenues à la carte SIM du terminal MS. La validité de la réponse SRES fournie par la carte au réseau atteste que l'intégrité du nombre aléatoire NA et des données DATA a été préservée, et empêche tout dénis  
35 de service. La confidentialité est assurée par l'association des données DATA au nombre aléatoire



NA, ce qui rend leur localisation difficile. L'invention permet donc de résoudre les problèmes soulevés précédemment en n'impliquant qu'une modification du logiciel des cartes SIM, les  
5 premières entités, et des enregistreurs nominaux et centres d'authentification, compris dans les deuxièmes entités, sans avoir aucun impact sur l'infrastructure du réseau. Ces modifications peuvent être effectuées de manière graduelle sans  
10 bouleversement du réseau fixe.

Dans le procédé, le nombre aléatoire (NA) et les données (DATA) peuvent respectivement avoir Q bits et P-Q bits de longueur, P étant un entier constant.

15

Le procédé peut comprendre une étape de chiffrement des données (DATA) ou du couple formé par le nombre aléatoire (NA) et les données (DATA). Dans ce cas, la confidentialité des données DATA est  
20 accrue, ainsi que la résistance du système à des attaques de cryptanalyse.

Dans le procédé, un moyen d'authentification et d'enregistrement d'identité de terminal (VLR, HLR, AUC) peut déterminer plusieurs triplets comprenant  
25 chacun un nombre aléatoire (NA) les données (DATA) et un résultat de réponse (RSRES) correspondant au nombre aléatoire (NA) et aux données (DATA).

Le procédé peut comprendre une étape de déterminer (E8) une clé de chiffrement (Kc) en fonction du nombre aléatoire (NA), des données (DATA) et de la clé (Ki) dans la seconde entité (VLR, HLR, AUC).

35

Le procédé peut également comprendre une étape de ne déterminer (E10) une clé de chiffrement (Kc) en fonction du nombre aléatoire (NA), des données (DATA) et de la clé (Ki) dans la première entité (MS) que  
5 lorsque la réponse (SRES) et le résultat de réponse (RSRES) comparés sont identiques.

Enfin, dans le procédé, les données (DATA) peuvent être utilisées dans la première entité (MS)  
10 par une application de gestion de compte prépayé, pour mettre à jour des droits d'accès à des fichiers (DF, EF) mémorisés dans la première entité ou par une application pour activer une clé additionnelle (Ki'), dans le cas où une ou plusieurs clés additionnelles  
15 Ki' ont été mémorisées dans les première et deuxième entités.

L'invention concerne également un module d'identité (SIM) dans une première entité (MS) qui  
20 est caractérisé en ce qu'il comprend des moyens (ROM, EEPROM) pour mémoriser un algorithme (AA) et une clé (Ki), des moyens pour recevoir un nombre aléatoire (NA) et des données (DATA) et des moyens (ROM, EEPROM, RAM) pour exécuter au moins l'étape (E6)  
25 d'appliquer la clé (Ki) le nombre aléatoire (NA) et les données (DATA) à l'algorithme (AA) conformément à l'invention.

Enfin l'invention concerne aussi un centre  
30 d'authentification (AUC) dans un réseau de télécommunication (RR) qui est caractérisé en ce qu'il comprend des moyens pour mémoriser un algorithme (AA) et une clé (Ki), des moyens pour sélectionner un nombre aléatoire (NA) et des données  
35 (DATA) et des moyens pour exécuter au moins l'étape (E6') d'appliquer la clé (Ki) le nombre aléatoire

(NA) et les données (DATA) à l'algorithme (AA) conformément à l'invention.

5 D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations préférées de l'invention en référence aux dessins annexés correspondants dans lesquels :

10 - la figure 1 est un bloc-diagramme schématique d'un réseau de radiotéléphonie cellulaire numérique ;

- la figure 2 montre schématiquement des étapes d'un procédé d'authentification d'un réseau de  
15 radiotéléphonie cellulaire numérique ; et

- la figure 3 montre des étapes d'une transmission sécurisée de données selon l'invention ;

20 Le procédé de l'invention est décrit ci-après dans le cadre du réseau de radiotéléphonie RR de type GSM, déjà présenté en référence à la figure 1, qui ne subit que des modifications et adjonctions de logiciel essentiellement dans le centre  
25 d'authentification AUC, ainsi que dans les cartes SIM des terminaux mobiles.

Dans la description ci-après, un réseau fixe est considéré comme la chaîne d'entités rattachées au  
30 terminal radiotéléphonique mobile considéré MS depuis l'interface radio IR, comprenant la station de base BTS, le contrôleur de station BSC, le commutateur MSC avec l'enregistreur de localisation des visiteurs VLR, et le couple HLR-AUC.

Il est rappelé qu'un terminal radiotéléphonique mobile MS d'un abonné comprend un module à microprocesseur amovible, dite carte à puce SIM reliée à un bus du circuit numérique à microprocesseur dans le terminal, le bus desservant le clavier, l'écran et des prises de périphérique du terminal mobile. Comme montré à la figure 1, la carte à puce SIM contient principalement un microprocesseur, une mémoire ROM incluant le système d'exploitation de la carte et des algorithmes d'application spécifiques, une mémoire non volatile EEPROM qui contient toutes les caractéristiques liées à l'abonné telles que l'identité IMSI, le profil d'abonnement, la liste de numéros d'appelés avec leurs noms, des données de sécurité tels que clé et code confidentiel, etc., et une mémoire RAM servant au traitement des données à recevoir du et à transmettre vers le circuit numérique du terminal. En particulier, les algorithmes d'authentification et de détermination de clé de chiffrement et les clés et autres paramètres liés à ces algorithmes sont gérés et écrits dans les mémoires ROM et EEPROM.

En référence à la figure 2, le procédé de transmission d'information sécurisé selon l'invention succède à une mise en communication de la carte SIM du terminal radiotéléphonique MS avec le sous-réseau BTS, BSC, MSC et VLR inclus dans le réseau de radiotéléphonie RR et rattaché temporairement au terminal radiotéléphonique MS, et précède une détermination de clé de chiffrement.

Le procédé montré à la figure 2 comprend essentiellement des étapes de E0 à E11. Dans la figure 2, les étapes E0, E2, E6', E60, E20, E8 et E81 sont effectuées essentiellement dans le réseau fixe,

indépendamment de toute demande d'authentification, et au moins préalablement à la demande de l'authentification considérée à l'étape E3 selon la réalisation illustrée.

5

Initialement, à une étape E0, le terminal mobile est considéré avoir mémorisé dans les mémoires ROM et EEPROM de sa carte SIM, l'identité IMSI de celle-ci, c'est-à-dire l'identité de l'abonné possesseur de la  
10 carte SIM, le cas échéant l'identité temporaire TMSI de la carte attribuée par le commutateur de rattachement MSC, une clé d'authentification Ki avec un algorithme d'authentification AA pour authentifier le terminal MS par le réseau, un algorithme de  
15 détermination de clé de chiffrement AC, un algorithme de chiffrement/déchiffrement. Ces données initiales et algorithmes sont également mémorisés à l'étape initiale E0 dans le réseau fixe. Les clés Ki pour chaque abonné sont mémorisées dans le centre  
20 d'authentification AUC en correspondance avec l'identité d'abonné IMSI, l'identité temporaire n'étant attribuée que par l'enregistreur de localisation des visiteurs VLR relié au commutateur du service mobile MSC auquel est rattaché le terminal  
25 mobile MS. L'algorithme d'authentification AA et l'algorithme de détermination de clé de chiffrement AC sont mémorisés dans le centre d'authentification AUC, et l'algorithme de chiffrement/déchiffrement est installé dans la station de base BTS. Comme on le  
30 verra dans la suite, le centre d'authentification AUC fournit des triplets [(NA, DATA), RSRES, Kc] à l'enregistreur de localisation nominal HLR.

Lors d'une demande d'accès au service mobile par  
35 le terminal, par exemple après la mise en fonctionnement du terminal mobile MS, ou pour une

mise à jour de la localisation du terminal, ou  
préalablement à une communication téléphonique, ou  
périodiquement pour authentifier la carte SIM à la  
demande de l'enregistreur VLR, le terminal MS échange  
5 des signaux avec le sous-réseau de rattachement de  
manière à dédier au terminal MS un canal de  
communication et à déclarer par le terminal MS au  
sous-réseau l'identité de terminal en transmettant  
l'identité IMSI de la carte SIM du terminal à  
10 l'enregistreur de localisation des visiteurs VLR, ou  
le cas échéant l'identité temporaire TMSI avec  
l'identité de la zone de localisation LAI relatives à  
la dernière communication établie. Ces échanges pour  
dédier un canal au terminal MS sont illustrés d'une  
15 manière simplifiée par l'étape E1 dans la figure 2.

Préalablement, dans le centre AUC, un générateur  
pseudo-aléatoire fournit plusieurs nombres aléatoires  
NA à Q bits. Les données DATA à transmettre de façon  
20 sécurisée selon le procédé de l'invention sont  
combinées avec chaque nombre aléatoire NA à Q bits et  
les couples (NA, DATA) résultats de cette combinaison  
sont écrits dans l'enregistreur HLR en association  
avec l'identité IMSI de la carte SIM, et au moins un  
25 couple (NA, DATA) choisi par l'enregistreur HLR est  
transmis à l'enregistreur VLR auquel est rattaché le  
terminal à l'étape E20.

Les données DATA sont transmises à la carte SIM  
30 selon le procédé de l'invention lorsque  
l'enregistreur de localisation des visiteurs VLR  
décide de procéder à l'authentification de la carte  
SIM par le réseau fixe: le couple choisi (NA, DATA)  
est introduit successivement dans des messages de  
35 demande d'authentification à l'étape E3 transmis  
respectivement par le commutateur MSC, le contrôleur

BSC et enfin la station de base BTS vers le terminal mobile MS à travers l'interface radio IR.

Si les couples (NA, DATA) font P bits de longueur, l'entier P, avec  $P > Q$ , pourra être choisi de manière à ne pas modifier la longueur des messages d'authentification selon la norme en vigueur dans le réseau de radiotéléphonie RR, en l'occurrence la longueur des messages contenant un nombre RAND. Dans ce cas les modifications apportées au réseau RR et aux cartes SIM seront encore réduites. L'entier P est typiquement égal à 128, soit une taille du couple (NA, DATA) égale à 16 octets. L'entier Q dénotant le nombre de bits dans le nombre aléatoire NA peut être supérieur ou inférieur à  $P/2$  ; toutefois les entiers P et Q peuvent satisfaire l'égalité  $P/2 = Q$ .

Dans la carte SIM du terminal mobile MS, le nombre aléatoire NA et les données DATA sont écrits en mémoire RAM de la carte SIM à l'étape E4 en réponse aux messages de demande d'authentification transmis par la station de base de rattachement BTS.

A cet instant la carte SIM a reçu les données DATA et peut les utiliser dans une application particulière dont plusieurs exemples seront fournis par la suite.

Le nombre aléatoire NA et les données DATA reçus et la clé d'authentification Ki sont lus à l'étape E5 afin de les appliquer à l'algorithme d'authentification connu AA à l'étape E6. A ce stade, l'authentification se poursuit sensiblement comme dans une carte SIM connue. L'algorithme AA fournit une réponse signée SRES (Signed RESponse) qui est incluse dans un message transmis à la station de base

de rattachement BTS, laquelle la retransmet à l'enregistreur VLR à travers la station de base BTS, le contrôleur BCS et le commutateur MSC.

5           Au préalable, avant la demande d'authentification E3 et donc avant la réalisation des étapes E4 à E6 dans la carte SIM, les enregistreurs VLR et HLR ont mémorisé pour l'abonné le nombre NA et les données DATA, et le centre  
10 d'authentification AUC a appliqué, après l'étape E20, et pour chacun desdits nombres aléatoires NA, le couple (NA, DATA) et la clé Ki à l'algorithme AA à une étape E6'. L'algorithme AA produit un résultat de réponse signée RSRES pour chaque couple (NA, DATA).  
15 Concomitamment avec l'étape E20, les résultats RSRES sont écrits dans l'enregistreur HLR à une étape E60 et le couple (NA, DATA) choisi par l'enregistreur est transmis avec le résultat correspondant RSRES à l'enregistreur VLR qui les a mémorisés.

20

A réception de la réponse signée SRES transmise par le terminal mobile MS après l'étape E6, l'enregistreur VLR lit le résultat de réponse signée RSRES à l'étape E61 et le compare à la réponse reçue  
25 SRES à l'étape E7. Si ces deux variables ne sont pas identiques, l'enregistreur VLR commande au commutateur de rattachement MSC de déconnecter le terminal et le réseau fixe à l'étape E71, empêchant le terminal de poursuivre sa demande d'accès au  
30 service mobile.

Dans le cas contraire, le centre d'authentification AUC valide l'authentification de la carte SIM à l'étape E7, pour autoriser le  
35 chiffrement et le déchiffrement des messages échangés



ultérieurement entre le terminal mobile MS et le sous-réseau BTS-BSC-MS.

5 A cet instant, le centre d'authentification AUC a non seulement authentifié la carte SIM, mais il a également la preuve que celle-ci a bien reçu les données DATA.

10 L'association des données DATA au nombre aléatoire NA peut avoir comme conséquence une relative diminution de la résistance du couple (NA, DATA) aux attaques de cryptanalyse par rapport à un nombre aléatoire de même dimension. Dans le but d'atténuer cet effet, un chiffrement des données DATA  
15 ou du couple (NA, DATA) peut être effectué par le centre d'authentification AUC avant leur transmission vers la carte SIM. Une telle étape de chiffrement aura également comme conséquence d'améliorer notablement la confidentialité des données DATA  
20 transmises.

La réponse signée SRES que la carte SIM envoie au réseau pour s'authentifier est généralement beaucoup plus courte que le nombre aléatoire RAND ou  
25 le couple (NA, DATA) transmis par le réseau à la carte SIM. Néanmoins, des données peuvent également être associées à la réponse signée SRES ou insérées dans celle-ci, de façon à permettre à la carte SIM de communiquer des informations au réseau RR. Même si la  
30 quantité d'informations transmises est très limitée, elle suffit à signaler au réseau un comportement révélateur de fraudes.

35 Une fois les données DATA reçues par la carte SIM et l'authentification de la carte SIM vérifiée par le centre d'authentification AUC, une clé de

chiffrement Kc peut alors être déterminée : au préalable, le centre d'authentification AUC a appliqué les couples (NA, DATA) correspondant auxdits plusieurs nombres aléatoires NC et la clé Ki à l'algorithme de détermination de clé de chiffrement AC à une étape E8 afin de produire des clés de chiffrement Kc, qui sont mémorisées dans l'enregistreur VLR à une étape E81 concomitante aux étapes E20 et E60. Ainsi, plusieurs triplets [(NA, DATA), RSRES, Kc] sont mémorisés préalablement dans l'enregistreur de localisation nominal HRL, et au moins l'un d'eux choisi est écrit dans l'enregistreur VLR en association avec l'identité IMSI/TMSI de la carte SIM.

15

A la suite de l'étape E7, le commutateur MSC décide de passer en mode chiffré en transmettant un message d'autorisation de chiffrement avec la clé Kc, relayé par les entités BSC et BTS, vers le terminal mobile MS, la clé Kc étant prélevée par la station de base BTS.

20

Par ailleurs, à la suite de l'exécution de l'étape d'authentification E6, la carte SIM lit à l'étape E9 le couple nombre aléatoire NA et donnée DATA et également la clé d'authentification Ki afin de les appliquer à l'algorithme de chiffrement AC pour déterminer une clé de chiffrement Kc à l'étape E10.

25

Finalement à des étapes E11 et E11', le terminal MS et le sous-réseau de rattachement, particulièrement la station de base de rattachement BTS qui contient un algorithme de chiffrement et déchiffrement identique à celui contenu dans la carte SIM et qui a mémorisé la clé déterminée Kc, peuvent

30

35

échanger des messages chiffrés et déchiffrés avec la clé Kc.

Premier exemple de mise en oeuvre du procédé selon l'invention: sécurisation de réseaux de radio-télécommunication fonctionnant en mode prépayé

Certains réseaux de télécommunication utilisent le mode de fonctionnement prépayé suivant : chaque fois que l'utilisateur du terminal mobile MS désire approvisionner son compte il se rend à un terminal de paiement effectue une transaction pour une certaine valeur. Une fois la transaction validée par un service bancaire, le réseau RR envoie à la carte SIM des informations dans le but de mettre à jour dans la carte un compteur ACM (Accumulated Card Meter) et la valeur maximale ACMmax que ce compteur peut atteindre, au moyen d'un message SMS. Ensuite lors de chaque communication, le réseau RR envoie au terminal mobile MS une information de tarification CAI (Charge Advice Information), que le terminal MS utilise pour envoyer à la carte SIM des commande d'incrémentations du compteur ACM. Grâce à des échanges avec la carte SIM, le terminal MS vérifie régulièrement que le compteur ACM ne dépasse pas sa valeur maximale permise ACMmax.

Malheureusement, comme les échanges entre le terminal mobile MS et la carte SIM ne sont pas sécurisés, un tel système est assez facile à pirater.

Grâce au procédé de transmission sécurisée de données selon l'invention, il devient possible de transmettre à la carte SIM, de façon sécurisée, des informations de début et de fin de communication et/ou des données d'estimation de la fréquence des

augmentations du compteur ACM. La carte SIM est alors capable de détecter les tentatives de fraudes de façon autonome et de prendre des mesures appropriées.

5        Second exemple de mise en oeuvre du procédé selon l'invention : modification de la carte SIM.

      Une modification de la carte SIM peut être nécessaire dans de nombreux cas. Par exemple en cas  
10 de détection par le réseau de tentatives de fraude, le réseau peut envoyer à la carte une commande de blocage temporaire ou permanent. Lors d'ajout ou de suppression de services, le procédé de transmission sécurisée de données selon l'invention permet de  
15 modifier les droits d'accès à des fichiers élémentaires EF (Elementary Files) ou à des fichiers dédiés DF (Dedicated Files) contenant par exemple des scripts de commande SIMToolkit ou  $\mu$ combo.

20        Troisième exemple de mise en oeuvre du procédé selon l'invention : modification urgente d'une clé.

      Les cartes SIM contiennent de nombreuses clés qui peuvent servir pour différentes applications. Ces  
25 clés sont généralement mémorisées dans la carte SIM lors de sa phase de personnalisation. En utilisant le procédé de transmission selon l'invention, et en mémorisant dans la carte SIM une ou des clés de rechange, il suffit d'envoyer une commande de  
30 commutation de clé pour passer de l'utilisation d'une clé compromise, c'est à dire rendue publique, à l'utilisation d'une clé de rechange toujours secrète.

      Bien que l'invention ait été décrite selon des  
35 réalisations préférées en référence à un réseau de radiotéléphonie entre un terminal radiotéléphonique

mobile et le réseau fixe du réseau de radiotéléphonie, le procédé d'authentification de l'invention peut être mis en oeuvre dans un réseau de télécommunication relativement à deux entités  
5 quelconques qui dans laquelle la première entité authentifie la seconde au moyen d'un mécanisme de challenge aléatoire / réponse signée.

## REVENDICATIONS

1 - Procédé de transmission sécurisée de données (DATA) entre une première entité (MS) et une deuxième entité (VLR, HLR, AUC) dans un réseau de télécommunication (RR), comprenant une étape d'authentification de la première entité (MS) par la seconde entité (VLR, HLR, AUC), ladite étape d'authentification comprenant des étapes (E6, E6') d'appliquer une clé (Ki) mémorisée dans les première et deuxième entités et un nombre aléatoire (NA) produit par la deuxième entité et transmis par la deuxième entité à la première entité à des algorithmes identiques (AA) mémorisés dans les première et deuxième entités, et comparer (E7) dans la deuxième entité (VLR, HLR, AUC) une réponse (SRES) produite par l'algorithme (AA) mémorisé dans la première entité et transmise à la deuxième entité et un résultat de réponse (RSRES) produit par l'algorithme (AA) mémorisé dans la deuxième entité, caractérisé par les étapes de :

transmettre de la deuxième entité à la première entité les données (DATA) avec le nombre aléatoire (NA), appliquer les données (DATA) avec le nombre aléatoire (NA) à l'algorithme (AA) dans la première entité et dans la seconde entité.

2 - Procédé conforme à la revendication 1 selon lequel le nombre aléatoire (NA) et les données (DATA) ont respectivement Q bits et P-Q bits de longueur, P étant un entier constant.

3 - Procédé conforme à la revendication 1 ou 2 caractérisé par une étape de chiffrement des données

(DATA) ou du couple formé par le nombre aléatoire (NA) et les données (DATA).

4 - Procédé conforme à l'une des revendications précédentes, caractérisé en ce qu'un moyen d'authentification et d'enregistrement d'identité de terminal (VLR, HLR, AUC) détermine plusieurs triplets comprenant chacun un nombre aléatoire (NA) les données (DATA) et un résultat de réponse (RSRES) correspondant au nombre aléatoire (NA) et aux données (DATA).

5 - Procédé conforme à la revendication 4, comprenant une étape de déterminer (E8) une clé de chiffrement (Kc) en fonction du nombre aléatoire (NA), des données (DATA) et de la clé (Ki) dans la seconde entité (VLR, HLR, AUC).

6 - Procédé conforme à l'une des revendications 4 ou 5, comprenant une étape de ne déterminer (E10) une clé de chiffrement (Kc) en fonction du nombre aléatoire (NA), des données (DATA) et de la clé (Ki) dans la première entité (MS) que lorsque la réponse (SRES) et le résultat de réponse (RSRES) comparés sont identiques.

7 - Procédé selon l'une des revendications précédentes, caractérisé en ce que les données (DATA) sont utilisées dans la première entité (MS) par une application de gestion de compte prépayé.

8 - Procédé selon l'une des revendications précédentes, caractérisé en ce que les données (DATA) sont utilisées dans la première entité (MS) pour mettre à jour des droits d'accès à des fichiers (DF, EF) mémorisés dans la première entité.

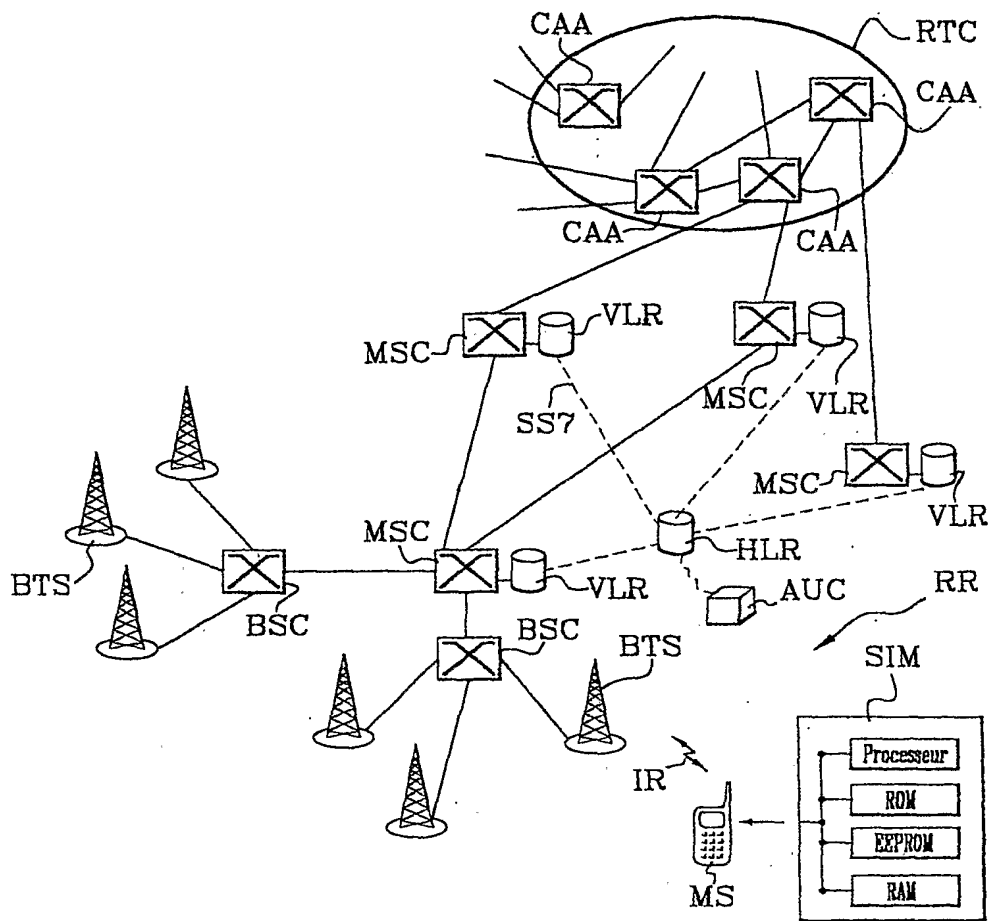
9 - Procédé selon l'une des revendications précédentes, caractérisé en ce que une ou plusieurs clés additionnelles  $K_i'$  sont mémorisées dans les première et deuxième entités, et en ce que les données (DATA) sont utilisées dans la première entité (MS) par une application pour activer une clé additionnelle ( $K_i'$ ).

10 10 - Module d'identité (SIM) dans une première entité (MS) caractérisé en ce qu'il comprend des moyens (ROM, EEPROM) pour mémoriser un algorithme (AA) et une clé ( $K_i$ ), des moyens pour recevoir un nombre aléatoire (NA) et des données (DATA) et des  
15 moyens (ROM, EEPROM, RAM) pour exécuter au moins l'étape (E6) d'appliquer la clé ( $K_i$ ) le nombre aléatoire (NA) et les données (DATA) à l'algorithme (AA).

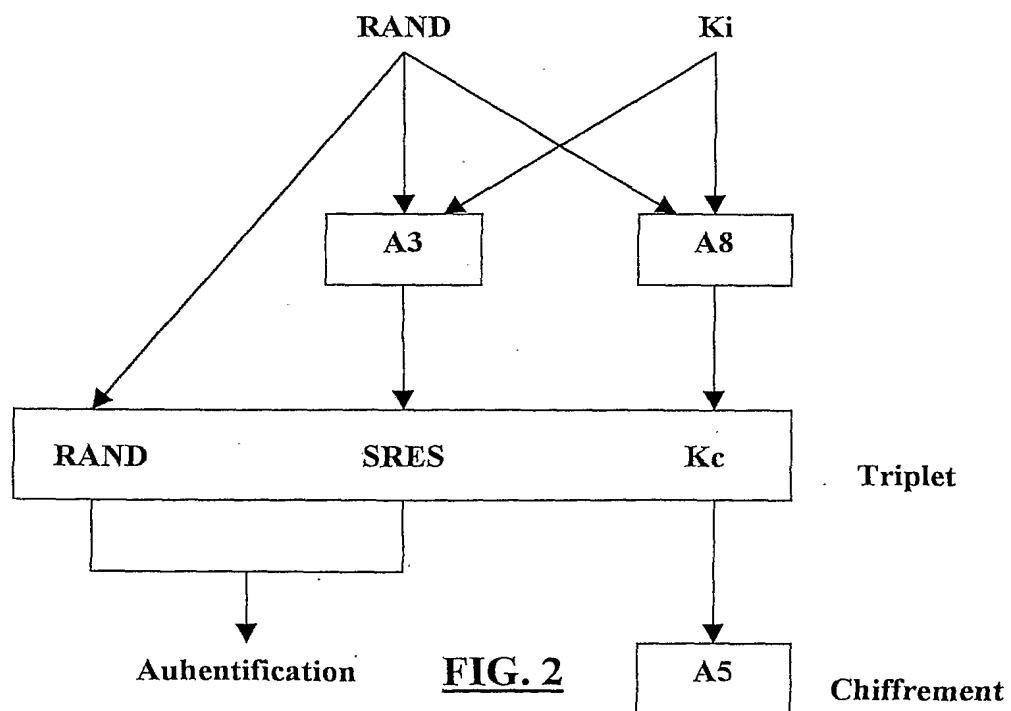
20 11 - Centre d'authentification (AUC) dans un réseau de télécommunication (RR) caractérisé en ce qu'il comprend des moyens pour mémoriser un algorithme (AA) et une clé ( $K_i$ ), des moyens pour sélectionner un nombre aléatoire (NA) et des données  
25 (DATA) et des moyens pour exécuter au moins l'étape (E6') d'appliquer la clé ( $K_i$ ) le nombre aléatoire (NA) et les données (DATA) à l'algorithme (AA).



1/2



**FIG. 1**



**FIG. 2**

2/2

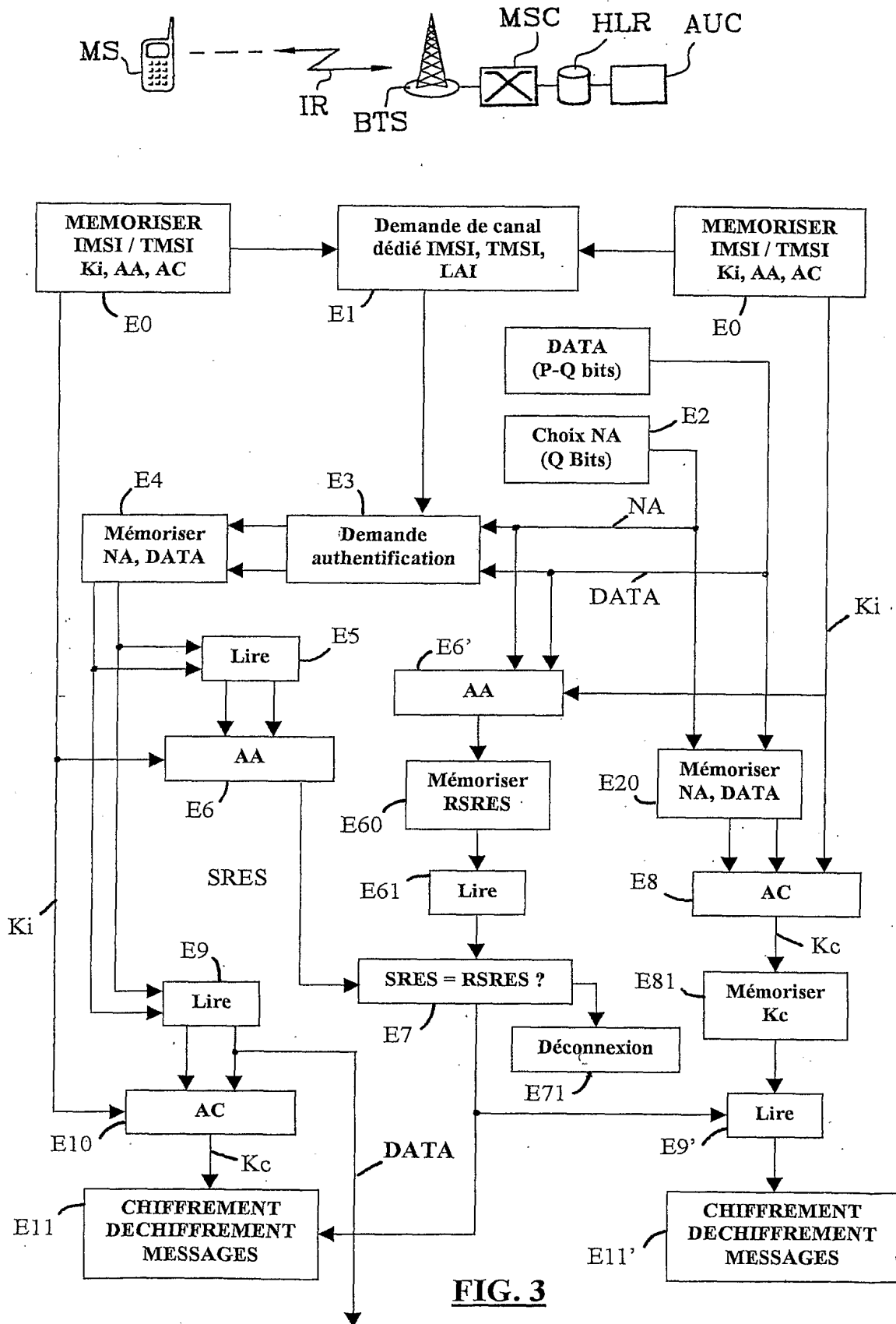


FIG. 3